NORTON ROSE FULBRIGHT

US data privacy policy

August 2020

Contents

Clause **Page**

Contents 1

Data Protection Policy 2

1 Policy Statement 2

2 Introduction 2

3 Privacy and Data Protection 2

3.1 What is data protection? 2

3.2 Why is data protection important? 3

3.3 How does it affect me? 3

4 Security, Integrity and Confidentiality 4

5 Medical and Other PHI 5

6 Marketing Requirements 5

7 Sharing Data with Third Parties 6

8 Complaints 7

9 Audit 7

Definitions 7

Special Provisions for HIPAA-Covered Information 8

Data Protection Complaints Procedure 20

Managing Data Subject Access Requests 21

Initial receipt and acknowledgment of request 21

Identifying and retrieving relevant information 22

Review of information 22

Response to the applicant 22

Managing follow-up queries 23

California Privacy Notice - All California Personnel 24

Background/purpose 24

Policy 24

Data Protection Policy

1 Policy Statement

Norton Rose Fulbright US LLP handles a vast amount of data each day to carry out its business and provide its services. This includes information about our people and the individuals with whom we conduct business, including contacts and employees at current, past and prospective clients and suppliers.

This policy represents a commitment that the firm will comply with all data privacy requirements applicable to it.

2 Introduction

As part of our legal practice, we will routinely need to collect, use, share or disclose information about our clients, people and the suppliers of various services for business purposes. We appreciate that the use and disclosure of such information has important implications for the firm and for the individuals concerned.

In the U.S., states have long required attorneys to keep client information confidential, but states are now beginning to enact data protection laws, including the California Consumer Privacy Act. Sometimes, the firm is subject to data privacy obligations due to the nature of the client, such as a hospital (subject to HIPAA, so the firm may be a "business associate"). In addition, some clients require that we maintain their data solely within the U.S. This policy is designed to ensure compliance with all data privacy requirements applicable to it.

Capitalized words included in this policy are as defined in Appendix 1. (For California-based employees, please also see the California Personnel Data Privacy Notice.)

If you have any questions or concerns about how this policy operates, please contact Rebecca Reason Hammond, Chief Administrative Officer and the firm's Data Protection Officer, at rebecca.hammond@nortonrosefulbright.com.

3 Privacy and Data Protection

3.1 What is data protection?

In essence, data protection is about protecting Personal Data and ensuring that privacy rights are respected when Personal Data is Processed by a business.

The scope of information classified as Personal Data (*any information relating to an identified or identifiable person*) is very broad. Sometimes it will be obvious when information is Personal Data and in other circumstances it will be less clear. Individuals can be identified by various means including their name and address, telephone number or email address. As an additional general rule, if information is obviously about, clearly linked or related to, or has as its main focus on an individual, it will almost certainly be Personal Data. For example:

(a) Employee ID numbers, employment and education history details and appraisal outcomes are Personal Data;

(b) Information such as age, gender and salary could be Personal Data when combined even if they are not directly linked to an individual's name; and

(c) Opinions and expressions of intentions about individuals are Personal Data.

Personal Data covers information processed automatically and in a structured manual (hard copy) filing system. "Processed automatically" includes not only information held on, or relating to the use of, a computer, laptop, mobile phone or similar device but also information derived from CCTV or electronic door or access passes.

Under data protection laws, some types of information such as medical history/health information are subject to additional protection and more stringent rules apply as explained later in this Policy.

3.2 Why is data protection important?

The firm will always be legally responsible for data protection compliance. Handling Personal Data in accordance with this Policy will allow the firm to operate effectively using the Personal Data of its partners, employees, clients, and suppliers without exposing these individuals to the risk of personal embarrassment, fraud, identity theft or unwarranted discrimination. Failure to manage Personal Data correctly and in accordance with this policy may have a number of negative consequences. Non-compliance could result in issues with:

Reputation: loss of trust and confidence of our people, clients and other business partners. Everyone who deals with the firm must have confidence in its ability to manage Personal Data in an appropriate manner.

Legal action/significant fines: prosecution (including for individuals) or other enforcement action from regulators.

Breach of contract: we have express obligations under some of our terms of contracts with clients and suppliers, which require us to handle Personal Data in certain ways.

Costs: increased costs of operating the firm's business.

3.3 How does it affect me?

This policy applies to all Norton Rose Fulbright US LLP personnel, including temporary and contract employees. Each of us will frequently Process Personal Data when performing our respective roles. Everyone in the firm, therefore, needs to understand their responsibilities and the rules that apply to the handling of Personal Data. Each of us has an important role to play in maintaining the firm's data protection compliance.

If you believe that this policy has not been followed in respect of Personal Data about yourself or someone else, you should promptly raise this with your line manager or the firm's Data Protection Officer.

Any breach of this policy, including in relation to misuse of Personal Data, will be taken seriously and may be considered as gross misconduct resulting in disciplinary action, including dismissal or other sanctions. In certain jurisdictions, a breach of data protection rules may also amount to a criminal offense.

Personal Data should not be kept longer than is necessary for the purpose for which it is being Processed. This means that Personal Data should be archived or erased (where possible) from our systems when it is no longer required.

The legal and business reasons the firm holds data should be considered when determining the required length of retention. Categories of information relating to firm personnel will have differing factors driving retention than information relating to clients and suppliers. Personal Data that forms part of a client file, for example, will need to be held for at least the minimum number of years required by relevant statutory provisions such as limitation periods or other local law requirements.

The firm will maintain retention policies and procedures to ensure that Personal Data is deleted after a reasonable time for the purpose for which it is being held, unless a law requires the data to be kept for a minimum time.

4 Security, Integrity and Confidentiality

Comply with our Global Cyber Security Policy

The firm must ensure that appropriate security measures are taken against unlawful or unauthorized processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. The firm has implemented various technical and organizational controls to ensure the security of its information assets (including Personal Data) as outlined in the Global Cyber Security Policy. Everyone in the firm **must** familiarize themselves with this policy and follow all procedures and technologies we put in place to maintain the security of Personal Data from the point of collection to the point of destruction.

Report breaches of this policy or Personal Data incidents without delay.

The firm may need to notify data protection regulators or its clients or employees of Personal Data incidents. Timescales for reporting such incidents vary, but it is essential that the following types of incidents are reported to the IT Service Desk and Data Protection Officer **immediately**:

(a) any unauthorized disclosure (**including emails sent to an incorrect recipient**) of the firm's corporate or personal information relating to employees, clients or suppliers;

(b) loss or theft of documents or storage media (laptops, USBs, phones etc.) containing corporate or personal information; or

(c) actual or attempted unauthorized access to systems or documents.

This includes events when you are traveling and thefts from your home.

When reporting an incident, please provide the following information:

(a) when the incident occurred and what happened (if the Personal Data was stolen, damaged, accidentally or deliberately disclosed, or otherwise accessed);

(b) the type of Personal Data affected (please provide as much detail as you can about the nature and sensitivity, the data fields and volume of records potentially affected);

(c) who the Personal Data relates to (clients, people within the Practice, or other third parties);

(d) the security measures applied, if any (for example if the Personal Data was encrypted);

(e) who else knows about the incident (individuals affected, others within the Practice, media, data protection regulators); and

(f) whether any steps have been taken to contain the incident and/or limit its impact (for example, trying to prevent the Personal Data being more widely disclosed or closing the point of weakness that allowed the incident to occur).

The matter should otherwise be kept strictly confidential.

Report supplier incidents

When you are informed of data protection incidents relating to anyone in the firm, clients or suppliers by any suppliers, you must immediately report such incidents to the IT Service Desk and Data Protection Officer.

All Personal Data incidents must be documented.

The firm maintains a register which contains information regarding all Personal Data incidents. If you report an incident, you should also provide an update to the Data Protection Officer on remediation measures that have been put in place after the Personal Data incident. The Data Protection Officer is responsible for completing the register with that information.

5 Medical and Other PHI

Some of the firm's clients are subject to HIPAA and engage the firm in matters that involve the firm's access to protected health information ("PHI"). It is the firm's policy to minimize its processing of PHI as much as possible. There will be instances, however, where we will hold this type of information (for example where it is directly relevant to a matter on which the firm is instructed). In such instances, PHI should be kept for as short a period as practical with restricted access permissions, and the information must only be used for the purposes for which it was provided. Where PHI forms part of a client/matter file, information barriers must be put in place to ensure that only those individuals who are working on the matter are able to access this information. *See the Attachment for the special provisions that relate to the requirements for PHI under HIPAA.*

6 Marketing Requirements

If the firm wishes to use contact information for direct marketing purposes, we will take reasonable steps when collecting the information to ensure that we do not collect any personally identifiable information. The firm's best practices for email marketing include:

(a) Sending marketing emails via Vuture using our InterAction preference lists;

(b) Including the ability for individuals to update their preferences or unsubscribe in order to opt out; and

(c) Removing contracts from our mailing lists that have not engaged with the firm in over 12 months to ensure we are not spamming inactive accounts.

When personally identifiable information that is not business-related, such as a birthday or home address, is required for something, that information will not be saved to the contact's record in InterAction. It will be saved on an event list that will be removed from InterAction when it's no longer required.

Particular care should be taken when organizing joint events or when we are looking to invite the firm's client/business contacts to an event hosted or managed by an external third party. We are not permitted to simply share the details of contacts with such a third party. Instead, we should either:

(a) Send the event invite ourselves (informing contacts, if not clear from the invite itself, that their details will need to be shared with the other party where they accept); or,

(b) In exceptional circumstances and as an absolute minimum, send an initial email informing contacts about the event and the intention of sharing their details with the third party managing the event (and its registration process) to allow contacts an opportunity to object to their details being shared with that third party.

Please contact the Data Protection Officer or our Marketing Database Manager if you have any questions related to marketing.

7 Sharing Data with Third Parties

The firm is committed to keeping Personal Data secure. When Personal Data is within our organization, we provide policies, training and other awareness measures to facilitate responsible and compliant data handling. There will be occasions, however, when it may be necessary to transfer Personal Data to third parties as part of a business support or outsourcing arrangement. This may include companies contracted to make travel arrangements, provide technology, hosting or other IT related services, or to assist the firm with ancillary services such as pension administration.

Initial key considerations

Prior to any data sharing, we must initially consider:

(a) What is the scope and purpose of the data sharing – we cannot adequately assess the firm's duties if it is not clear what types of data may be shared and for what purpose;

(b) Would Data Subjects anticipate the sharing – we need to understand the source of the data, whether there are any restrictions on sharing, and whether the Data Subjects have been notified of or would anticipate the sharing; and

(c) Is the sharing really necessary for the purpose – we must share no more Personal Data than is necessary for the purpose. This is a data protection law requirement and also helps reduce the potential risk of data being mishandled.

Once the above is clear, we must take the necessary steps to on-board the third party.

Be cautious with telephone inquiries and other disclosure requests

Everyone must be careful about disclosing Personal Data held by the firm when dealing with telephone inquiries or other similar requests. You should never feel pressured into disclosing Personal Data. It is important to:

(a) Check the caller's or requestor's identity and right to know to make sure that Personal Data is only shared with someone who is entitled to receive it; and

(b) Require that the caller/requestor put the request in writing.

Please contact the Data Protection Officer for guidance if you have any questions or for assistance in difficult situations.

8 Complaints

The firm will treat any concerns or complaints regarding its processing of Personal Data as a matter of urgency.

If you are contacted by a complainant, you should promptly notify the firm's Data Protection Officer, who will deal with any such matter in line with the firm's Data Protection Complaints Procedure.

As indicated in this procedure, whenever data protection concerns are raised, the firm's approach is to engage positively to try to resolve a complaint satisfactorily without the individual needing to escalate matters or having to refer their complaint to an external data protection regulator or court.

9 Audit

In line with good practice, our Data Protection Officer will also periodically assess compliance with this policy, either as part of a wider audit undertaken by the Compliance team or a specific data protection audit of a practice group or business services team's processing activities.

Definitions

The following terms are used in this policy.

Personal Data is any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified (either directly or indirectly) by reference to an identifier. These include name, ID numbers, location data, online identifiers or one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person.

PHI. Data concerning health covers Personal Data relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual received from or on behalf of clients, or created for such clients, covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Special Provisions for HIPAA-Covered Information

HANDLING OF PHI

A. Use and Disclosure of PHI

The firm may not use or disclose PHI, except as permitted herein. The firm's employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the firm, is under the direct control of the firm, whether or not they are paid by the firm ("workforce") members may use or disclose PHI as set forth in the terms of a business associate agreement between the firm and any client that is a covered entity, defined by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulation ("HIPAA")to mean any healthcare provider transacting in electronic protected health information ("ePHI"), any health plan, and any health care clearinghouse. The firm may not use or disclose PHI in a manner that would violate HIPAA requirements if done by a firm client that is a covered entity.

1. The firm shall disclose PHI when required by the U.S. Department of Health and Human Services ("HHS") to investigate or determine the firm's compliance with HIPAA requirements.

2. The firm shall disclose PHI to a firm client that is a covered entity, an individual, or individual's designee, as necessary to satisfy the client's obligations with respect to the provision of electronic copies of PHI at an individual's request.

3. The firm shall not sell PHI except pursuant to and in compliance with an individual's authorization. The sale of PHI means a disclosure of PHI by the firm where it directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

B. Minimum Necessary

The firm will limit any use, disclosure or request for PHI to the limited data set, as set forth in the HIPAA Privacy Rule, or if needed by the firm, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

1. The firm workforce members shall use the minimum amount of PHI necessary to carry out job functions and shall disclose or request the minimum PHI needed to achieve the purpose of the disclosure or request. The firm's workforce members who routinely use, receive or request disclosure of PHI shall receive training on the firm's policies and procedures regarding minimum necessary disclosures.

2. Minimum necessary requirements do not apply to the following transactions:

    a. Disclosures to or requests by a health care provider for treatment;

    b. Uses or disclosures made to the individual who is the subject of PHI, as permitted under HIPAA or as may be required on the individual's request;

    c. Uses or disclosures made pursuant to a valid authorization from the individual who is the subject of PHI;

    d. Disclosures made to HHS as part of a compliance investigation;

e. Uses or disclosures that are required by law; and

f. Uses or disclosures that are required for compliance with the HIPAA Privacy Rule.

3. The firm will identify the persons or classes of persons in its workforce who need to access PHI for their job functions and the category or categories of PHI to which each person or class of persons needs access. The Privacy Officer's designee will be responsible for maintaining documentation of the personnel by job function or class who need access to PHI and the types of PHI to which they need access. The firm will take reasonable efforts to limit access to PHI as specified in the documentation described herein.

4. The firm's workforce members who access PHI in order to do their jobs may not share that information with other workforce members, unless the recipients need to know that information by virtue of their duties with respect to the firm.

5. Accessing any PHI other than as required in the performance of the firm's duties is a violation of this policy and may result in disciplinary action up to and including involuntary termination.

6. The firm will limit the PHI it either requests or discloses from firm clients to that necessary to perform the specific legal services on behalf of the client designated in an agreement engaging the firm's services.

7. The firm may reasonably rely on the scope of the requested disclosure as the minimum necessary amount in the following situations:

   a. Requests by public officials as permitted by HIPAA, if the public official represents that the information requested is the minimum necessary for the stated purpose of the request;

   b. Requests by another HIPAA covered entity; or

   c. Requests by a subcontractor of the firm, performing services on behalf of a firm client pursuant to the terms of an agreement in which the subcontractor agrees to adhere to the same privacy and security requirements applicable to the firm as a business associate to the client and in which the subcontractor represents that the information requested is the minimum necessary for the stated purpose of the request.

8. The firm workforce members may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

C. Request for Privacy Restrictions

A firm client that is a covered entity may, from time to time, agree to an individual's request to restrict use or disclosure of PHI, in which case the client may not use or disclose restricted PHI except as permitted by the individual or as otherwise provided in the HIPAA Privacy Rule. To the extent that a firm client has agreed to such a restriction on the use or disclosure of PHI, and to the extent that the client has provided notice to the firm of such restriction, the firm shall abide by the terms of the restriction agreed upon by the client.

1. Any firm workforce member who receives an instruction from a firm client to restrict the use or disclosure of PHI shall provide such instruction to the firm Privacy Officer. Any firm workforce member who receives a request for restriction on the use or disclosure of PHI directly from an

individual who is the subject of PHI shall refer the request to the firm Privacy Officer, for treatment in accordance with an applicable business associate agreement. In the event that the business associate agreement so provides, the firm Privacy Officer shall refer the individual to the firm client that is a covered entity for determination as to whether the request for restriction will be granted. To the extent that a business associate agreement designates the firm as the primary contact for requests for restriction, the firm Privacy Officer, or his or her designee, shall make a determination as to whether the request must be honored pursuant to 45 CFR 164.522.

2. In the event that the firm agrees to a restriction on use or disclosure of PHI as addressed above, the firm will notify the appropriate firm client that is the covered entity.

3. The firm shall provide notice to the client that is a covered entity of any request for restriction on the use or disclosure of PHI within a reasonable time to permit the client to respond to the individual within sixty (60) calendar days after the request is received. In the event that the firm is the designated primary contact for requests for restriction, the firm shall respond to the individual within sixty (60) days, either agreeing to the requested restriction or denying the requested restriction. If the firm denies an individual's requested restriction, the firm Privacy Officer shall notify the individual in writing of this determination.

4. Any PHI that is the subject of an agreed-upon restriction shall be marked in an appropriate fashion so that the firm workforce members will be alerted to the nature of the restriction.

5. The firm shall inform all relevant the firm workforce members and subcontractors who use or disclose the restricted PHI of the restriction.

6. If the firm or a firm client that is a covered entity agrees to a restriction, the firm may still use or disclose the restricted PHI in conjunction with any request by HHS to review such PHI for compliance purposes.

7. To the extent that an individual terminates a restriction, that revocation of restriction shall be submitted to the firm in writing, either by the firm client having agreed to the initial restriction and revocation, or by the individual directly. The Privacy Officer's designee shall maintain a record of that terminated restriction. Whenever the firm receives an appropriately documented termination of restriction, such restriction will no longer apply to any PHI about that individual that the firm maintains.

8. If the firm has made an original agreement to restrict the use or disclosure of PHI (as opposed to a restriction agreed upon by the client), the firm may terminate an agreed-to restriction. If the individual agrees to terminate the restriction, the restriction will no longer apply to any of the PHI that the firm maintains, regardless of when created or received. If the individual does not agree to the termination, the restriction will continue to apply to PHI created or received before or while the restriction was in effect. However, new PHI created or received after the notice of termination will not be subject to the restriction.

9. The firm Privacy Officer and their designee shall ensure that the restrictions, if any, are documented and that such documentation is kept on file. Documentation of the restrictions shall be maintained for 6 years from the date the notation was made or 6 years from the date the restriction was last in effect, whichever is later.

D. De-Identification

Health information that does not identify an individual and for which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. Health information that meets the specifications under 45 CFR 164.514(a) and (b) is considered to be "de-identified." While the HIPAA Privacy Rule does not apply to information that has been de-identified as set forth herein, and thus may be used or disclosed without regard to the privacy restrictions addressed in this policy, the firm may de-identify client PHI and use or disclose accordingly only if permitted pursuant to the terms of an applicable business associate agreement. To the extent that the firm does de-identify information from a client, the firm may assign a code or other means of record identification to allow de-identified information to be re-identified by a recipient, provided that the code is not related to information about the individual and is not otherwise capable of being translated so as to identify the individual, and provided the recipient does not use the means of re-identification for any other purpose or disclose the means of re-identification.

E. Personal Representatives

Save for certain exceptions set forth herein, the firm must treat a personal representative of any individual who is the subject of PHI maintained, used or disclosed by the firm as the individual for purposes of compliance with the HIPAA Privacy Rule. The firm may elect not to treat a person as the personal representative of an individual (i) if the individual is an unemancipated minor able to consent to healthcare services; (ii) to the extent that the firm has a reasonable belief that an individual has been or may be subjected to domestic violence abuse, or neglect by a purported personal representative; or (iii) if treating such person as the personal representative could endanger the individual.

F. Whistleblowers

The firm shall not have violated the requirements of the HIPAA Privacy Rule if a member of the firm's workforce or a firm subcontractor discloses PHI, provided that (i) the workforce member or subcontractor believes in good faith that the firm has engaged in conduct that is unlawful or otherwise violates professional standards, or believes in good faith that that the services provided by the firm potentially endanger the public; and (ii) the disclosure is to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct of the firm or an attorney retained by or on behalf of the workforce member or subcontractor for the purpose of determining the legal options of the workforce member or subcontractor with regard to the conduct described herein.

G. Authorizations

Except as permitted by an applicable business associate agreement or under the HIPAA Privacy Rule, the firm shall not use or disclose PHI without first obtaining written authorization from an individual who is the subject of PHI. The firm recognizes that an individual may revoke an authorization at any time by submitting written notice to a client that is a covered entity or to the firm. Revocations become effective when received except to the extent that PHI has been created by a client or the firm to defend the client or the firm, respectively, in a legal action or other proceeding brought by the individual. All requests for disclosure requiring authorization shall be directed to the firm Privacy Officer. To the extent that a request is not accompanied by an authorization, the firm Privacy Officer shall direct the completion of authorization as appropriate. Once the firm has been provided with appropriate authorization, the firm Privacy Officer, or his or her designee, shall direct that the disclosure be made and shall maintain a file of all submitted authorization forms.

1. Authorization is required for certain uses or disclosures of PHI. The firm may not use or disclose PHI without an authorization in relation to the following purposes:

    a. Psychotherapy notes. The firm must obtain an authorization for any use or disclosure of psychotherapy notes, except for use by the originator of the psychotherapy notes for treatment, use or disclosure by the firm to defend a client or itself in a legal action or other proceeding brought by the individual who is the subject of psychotherapy notes, use or disclosure required by law, or use or disclosure for regulatory oversight purposes.

    b. Marketing. The firm must obtain an authorization for any use or disclosure of PHI for marketing purposes.

    c. Sale of PHI. The firm must obtain an authorization for any disclosure of PHI which is considered to be a sale of that PHI.

2. An individual may revoke an authorization at any time, provided that the revocation is in writing. Revocations of authorization shall be directed to the firm Privacy Officer. The Privacy Officer's designee shall maintain a record of all such revocations.

3. A valid authorization must contain the following:

    a. A description of the information to be used or disclosed;

    b. Identification of the persons, or class of persons, authorized to make the requested use or disclosure;

    c. Identification of the persons, or class of persons, to whom the firm may make the requested use or disclosure;

    d. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

    e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

    f. Signature of the individual and date; and

    g. Statements regarding the individual's right to revoke the authorization in writing, exceptions to that right, and how the individual may revoke authorization.

H. Request for Access

Subject to certain exceptions, an individual has a right of access to inspect and obtain a copy of his or her PHI held by the firm in a designated record set, for as long as the firm maintains the PHI. To the extent that the firm maintains PHI in a designated record set and at the request of a client who is a covered entity, or at the request of an individual directly, the firm shall provide access to PHI in a designated record set to the client or, as directed by the client, to an individual in order to meet the client's requirements under 45 CFR 164.524.

1. Any firm workforce member who receives a request for access to PHI from a firm client, or from an individual directly, shall forward such request to the firm Privacy Officer for treatment of that request in accordance with an applicable business associate agreement. In the event that the business associate agreement so provides, the firm Privacy Officer shall refer an individual to the client that is a covered entity for processing the request for access. To the extent that a business associate agreement designates the firm as the primary contact for requests for access, the firm Privacy Officer, or his or her designee, shall direct the provision of access to PHI by the firm.

2. The firm must provide an individual with access to PHI in the form and format requested by the individual if it is readily producible in such form and format or, if not, in a readable hard copy form or such other form and format as agreed to by the client or the firm, as appropriate, and the individual.

3. Individuals are entitled to copies of their PHI in an electronic form if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the firm client or the firm, as appropriate, and the individual. Individuals may direct the client or the firm, as appropriate, to transmit a copy of an electronic health record directly to a third party they designate clearly and specifically.

4. The firm requires that requests for access be in writing. To the extent that a request for access comes from a firm client, the firm shall require the client to submit its request for assistance in writing, a copy of which request shall be maintained by the Privacy Officer's designee. To the extent that a request comes from an individual directly, the firm shall request that the individual submit his or her request in writing, a copy of which request shall be maintained by the Privacy Officer's designee. The firm shall apply this policy uniformly.

5. To the extent that the firm has been designated as a primary contact for individuals seeking access to PHI pursuant to the terms of a business associate agreement, the firm may deny an individual's request for access.

    a. The firm may deny a request for access without providing the individual an opportunity for review when PHI was compiled by a firm client or the firm in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; when PHI consists of psychotherapy notes; or when PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

    b. The firm may deny a request for access, which denial may be reviewed, if a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access is reasonably likely to endanger the life or physical safety of the individual, is reasonably likely to cause substantial harm to another person, or if the request for access is made by the a personal representative of an individual and the provision of access is reasonably likely to cause substantial harm to the individual or another person.

    c. The firm shall provide a timely denial to the individual written in plain language and describing the basis for the denial. If the individual has a right to seek review of the firm's decision, the denial shall contain a statement regarding the right to review the decision, including a description of how the individual can exercise his or her rights, a description of how the individual may complain to the firm or to HHS, and the name and telephone number of the firm Privacy Officer.

6. If the firm denies an individual access to his or her PHI as described herein, the Individual has the right to have the denial reviewed by a licensed health care professional who is designated by the firm to act as a reviewing official and who did not participate in the original decision to deny access. The firm must provide or deny access in accordance with the determination of that official.

7. The firm shall verify the identity of any person requesting PHI and the authority of the person to have access to the PHI requested prior to granting access. The firm shall obtain any required written documentation from the client or individual, as appropriate, prior to granting access.

8. The firm shall either grant access as requested or provide written notice of denial within thirty (30) calendar days of the firm's receipt of request when the material requested is on-site at a firm facility. The firm shall either grant access as requested or provide written notice of denial within sixty (60) calendar days of the firm's receipt of request when the material requested is off-site. To the extent that the firm issues a denial, the firm shall provide the individual with access to any PHI requested for which the firm has not denied access.

9. If the firm cannot act on a request within the applicable deadline, it may extend the deadline by no more than thirty (30) calendar days by providing an individual with a written statement of the reasons for the delay and the date by which it will complete its action on the request. The firm must provide the written statement within the original time period and may only extend the time period once.

10. If a request for access pertains to PHI maintained in a designated record set by a firm subcontractor, the firm Privacy Officer, or his or her designee, will contact the subcontractor in order to obtain access to the requested PHI. If the firm has entered into an agreement with a subcontractor that designates the subcontractor as the primary contact for requests to access PHI, the firm Privacy Officer, or his or her designee, shall direct the individual to the subcontractor for access.

11. When providing access, the firm shall provide access to PHI in the form or format requested by the individual, if it is readily producible in this form or format; or if not, in a readable hard copy form or other form that is agreed upon by the firm and the individual (except to the extent required to be provided in electronic format). The firm may provide the a summary or explanation of the PHI instead of providing access to the actual PHI, to the extent that the firm and individual seeking access agree.

12. The firm may charge a reasonable, cost-based fee, provided that the fee includes only the cost of copying, postage, and preparing an explanation or summary of the PHI, if such summary is requested by the individual. Fees charged for an electronic copy will be limited to the firm's labor costs in responding to the request.

I. Request for Amendment

Subject to certain exceptions, an individual has a right to request amendment of PHI held by the firm in a designated record set, for as long as the firm maintains the PHI. To the extent that the firm maintains PHI in a designated record set, the firm agrees to make any amendments to PHI in a designated record set as directed or agreed to by a firm client who is a covered entity or the individual directly, as appropriate, in order to satisfy the client's obligations under 45 CFR 164.526. The firm Privacy Officer, or his or her designee, is responsible for directing the grant or denial of all requests for amendment and providing notice to the individual of the determination.

1. Any firm workforce member who receives a request for amendment of PHI from a firm client, or from an individual directly, shall forward such request to the firm Privacy Officer for treatment of that request in accordance with an applicable business associate agreement. In the event that the business associate agreement so provides, the firm Privacy Officer shall refer an individual to the client that is a covered entity for processing the request for amendment. To the extent that a business associate agreement designates the firm as the primary contact for requests for amendment, the firm Privacy Officer, or his or her designee, shall direct the provision of access to PHI by the firm.

2. The firm shall require that all requests to amend PHI must be in writing and include reasons to support the request. To the extent that an individual requests that the firm amend PHI outside of these requirements, the firm Privacy Officer or his or her designee shall inform the individual of the requirements for a request to amend PHI as set forth herein.

3. The firm may deny a request to amend an individual's PHI if it determines that the record that is the subject of the request was not created by the applicable client who is a covered entity or the firm, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment. The firm may also deny a request to amend an individual's PHI if it is not part of a designated record set, if it would not be otherwise available for inspection pursuant to 45 CFR 164.524, or if the firm determines that the record is accurate and complete. If the firm denies the requested amendment, in whole or in part, the firm must take the following steps:

    a. The firm must provide the individual with a written denial that includes the basis for the denial; a statement regarding how the individual may file a written disagreement; a statement permitting the individual to request that the firm provide the individual's request for amendment and denial with any future disclosures of the disputed PHI; and a statement regarding how the individual may make a complaint to the firm or to HHS.

    b. The firm must permit the individual to submit to the firm a written statement disagreeing with the denial and the basis for the disagreement. The firm may prepare a written rebuttal to the individual's statement of disagreement. If the firm prepares a rebuttal, it must provide a copy to the individual.

    c. The firm must identify, as appropriate, the PHI that is the subject of the disputed amendment and append or otherwise link to the individual's request for an amendment, the firm's denial of the request, the individual's statement of disagreement, and the firm's rebuttal to the information, if any.

    d. When making future disclosures of the disputed PHI, the firm must include either the material appended to the record, or an accurate summary of it, with any subsequent disclosure of the PHI to which the disagreement relates. However, if the individual has not submitted a written statement of disagreement, the firm shall include the appended information with any subsequent disclosure only if the individual has requested that the firm do so.

    e. Unless the firm determines, at the direction of the firm Privacy Officer, that a request for amendment should be denied for reasons set forth above, the firm shall make the appropriate amendment to the individual's PHI on record. The firm shall inform the individual on a timely basis that the amendment is accepted and obtain the individual's identification of, and agreement to have the firm notify, the relevant persons with whom the amendment needs to be shared.

4. The firm must act on a request for amendment within sixty (60) calendar days of receipt of the request. If the firm is unable to act on the amendment within sixty (60) calendar days, the firm may, on a one-time basis, extend by thirty (30) calendar days the time in which it may act, provided that notice is given within the original sixty (60) calendar day period regarding the reasons for the delay and the date by which the firm will complete its action on the request. After having made any amendment, the firm shall make reasonable efforts to inform and provide the amendment within reasonable time to persons identified by the individual as having received PHI and needing the amendment, and persons, including the client or any subcontractors, that the firm is aware of having the unamended information that may have relied, or might rely in the future, on the unamended information to the detriment of the individual.

5. If the firm receives notification from a covered entity that an individual's PHI has been amended, the firm Privacy Officer, or his or her designee, shall direct the amendment of that PHI in the firm's designated record set. The firm Privacy Officer shall also ensure that other appropriate persons, including any applicable clients or subcontractors, have been provided notice of such amendment.

6. The firm Privacy Officer shall be responsible for directing the receipt and processing of requests for amendment of PHI. All such requests shall be forwarded to the firm Privacy Officer upon receipt by any the firm workforce member. The firm Privacy Officer shall document and the Privacy Officer's designee shall maintain records of all requests for amendment and the resolution of those requests.

J. Accounting of Disclosures

Save for certain exceptions, an individual has a right to receive an accounting of all disclosures of his or her PHI made by a covered entity for the 6 year period prior to the date of the request. The firm shall document and maintain documentation of disclosures of PHI and make available to any firm client that is a covered entity information related to such disclosures as would be required for the client to respond to a request by an individual for such an accounting pursuant to 45 CFR 164.528.

1. Any firm workforce member who receives a request for an accounting of PHI disclosures from a firm client, or from an individual directly, shall forward such request to the firm Privacy Officer for treatment of that request in accordance with an applicable business associate agreement. In the event that the business associate agreement so provides, the firm Privacy Officer shall refer an individual to the firm client that is a covered entity for processing the request for accounting. To the extent that a business associate agreement designates the firm as the primary contact for requests for amendment, the firm Privacy Officer, or his or her designee, shall direct the provision of an accounting by the firm.

2. The firm is not required to provide an accounting of disclosures that were made in the following circumstances:

    a. To carry out treatment, payment and health care operations;

    b. To individuals, of PHI about them;

    c. Incident to a use or disclosure otherwise permitted or required by 45 CFR Part 164, Subpart E;

    d. Pursuant to an authorization provided by an individual;

e. To persons involved in the individual's care or other notification purposes related to an individual's right to object to disclosures of PHI;

f. For national security or intelligence purposes

g. To correctional institutions or law enforcement officials;

h. As part of a limited data set in accordance with the requirements set forth in 45 CFR 164.514(e); or

i. Occurring prior to the compliance date for the firm.

3. Under certain circumstances a health oversight agency or law enforcement official may request that the firm temporarily suspend an individual's right to receive an accounting of disclosures to the health oversight agency or law enforcement official.

   a. Upon appropriate request, the firm must temporarily suspend the individual's right to receive an accounting of these disclosures for the time specified by such agency or official, if such agency or official provides the firm with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities; and specifying the time period for which such a suspension is required.

   b. In the event that an agency or official statement is made verbally to the firm, the firm Privacy Officer must ensure that the statement is documented, including the identity of the agency or official making the statement. The firm shall temporarily suspend an individual's right to an accounting of disclosures in accordance with any such statement.

   c. The firm shall limit the temporary suspension to no longer than thirty (30) calendar days from the date of the verbal statement, unless a written statement from the agency or official is submitted during that time.

4. The firm will act on a request for an accounting no later than sixty (60) calendar days after receipt of such a request, in the following ways:

   a. The firm will provide the individual with the accounting requested.

   b. If the firm is unable to provide the accounting within sixty (60) calendar days of receipt of the request, the firm may extend the time to provide the accounting once, by no more than thirty (30) days, provided that the firm, within sixty (60) calendar days of receipt of the request, provides the individual with a written statement of the reasons for the delay and the date by which the firm will provide the accounting.

5. The firm shall provide the first accounting to an individual in any 12-month period without charge. The firm may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same Individual within the same 12-month period, provided that the firm informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

6. If a requested accounting covers disclosures of PHI that were made by a the firm subcontractor, the firm will confer with that subcontractor in order to obtain the information needed to provide an accounting of such disclosures, in accordance with the agreement between the firm and the subcontractor. If a requested accounting covers disclosures of PHI that were made by a

subcontractor of the firm, and that subcontractor has agreed in writing to be the primary point of contact for such requests, the firm will refer that individual to the subcontractor for provision of the accounting. The subcontractor will be responsible for providing the accounting in accordance with the HIPAA Privacy Rule and the business associate subcontract agreement with the firm.

7. An accounting of disclosures must be in writing and must contain the following elements for each disclosure:

    a. Date of the disclosure;

    b. The name of the entity or person who received the PHI;

    c. The address of the entity or person who received the PHI, if known;

    d. A brief description of the PHI disclosed;

    e. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's written authorization for disclosure, or a copy of a written request for a disclosure made pursuant to the firm's policy for disclosures to government entities.

8. The firm may provide a summary accounting for multiple disclosures if, during the period covered by the accounting, the firm has made multiple disclosures of PHI to the same recipient pursuant to a single authorization signed by an individual, for a single purpose to HHS so it may investigate or determine the firm's compliance with the HIPAA Privacy Rule, or to the same person or entity for a single national priority purpose. When providing a summary accounting, the firm may limit the accounting related to a series of disclosures to the core elements (set forth in section 7. above) for the first disclosure during the accounting period, along with the frequency or number of the disclosures made during the accounting period and the date of the most recent disclosure in the series during the accounting period.

9. The firm must create and maintain the following documentation:

    a. The core elements of each disclosure as set forth in section 7 above;

    b. The written accounting that is provided to the individual

    c. The titles of the persons or offices within the firm responsible for receiving and processing an individual's request for an accounting.

K. Compliance Reviews

1. **Complaints**. A person who believes that the firm is not complying with HIPAA requirements may file a complaint with the Secretary of HHS. Complaints under this section must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the firm's HIPAA requirements. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred.

2. **Cooperation with Compliance Review**. The firm must cooperate with HHS, if it undertakes an investigation or compliance review of the firm policies, procedures, or practices to determine whether it is complying with the applicable HIPAA requirements. The firm must keep such

records and submit such compliance reports, in such time and manner and containing such information, as HHS may determine to be necessary to enable the Secretary to ascertain whether the firm has complied or is complying with applicable HIPAA requirements.

a. The firm, at the direction of the firm Privacy Officer, must permit HHS to access the firm's facilities, books, records, accounts, and other sources of information, including protected health information ("PHI") during normal business hours, to the extent that such information is pertinent to ascertaining compliance with the HIPAA requirements applicable to the firm. If HHS determines that exigent circumstances exist, the firm shall permit access at any time and without notice.

b. If any information required of the firm is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the firm will so certify; the firm Privacy Officer shall provide HHS with a description of the efforts that the firm has made to obtain the information.

3. **Investigational Subpoenas**. HHS may issue subpoenas and require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review of the firm's activities. Any recipient of any such subpoena or request for testimony or documentation shall immediately provide copies of that subpoena or request to the firm's General Counsel and the firm Privacy Officer.

4. **Prohibition on Intimidation or Retaliation**. The firm and its employees are prohibited from threatening, intimidating, coercing, harassing discriminating against, or taking any other retaliatory action against any individual or other person for filing a complaint as described herein; for testifying, assisting, or participating in an HHS investigation, compliance review, proceeding, or hearing; or for opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

Data Protection Complaints Procedure

Norton Rose Fulbright US LLP (**the Firm**) is committed to protecting personal data and strives to meet the highest data privacy and information security standards. As such, the Firm will treat any concerns or complaints regarding its processing of personal data and/or non-compliance with its Data Protection Policy and California Personnel Privacy Notice as a matter of urgency and as outlined below.

The Firm recognizes that a complaint may relate to a number of different areas such as:

- unauthorized access to personal data
- misuse of personal data
- loss of personal data
- another type of breach of Norton Rose Fulbright's Data Protection Policy and California Personnel Privacy Notice

There are various routes through which a concern or problem about the way in which personal data is handled can be raised. A third party may initially speak to its/their regular contact at the Firm, for example their Client Relationship Manager, or an individual may liaise with their dedicated Human Resources or local data privacy contact where the complainant is a member of Firm personnel. A complainant will be asked to provide a full written explanation of the issue to assist in investigating the matter.

The details of the complaint will then be promptly forwarded to the Firm's Data Protection Officer for the United States (**DPO**), who will deal with the matter fairly and without delay. The DPO will acknowledge receipt of the complaint, confirm that the matter will be investigated, and provide an estimate of how long the individual should expect to wait until a response is provided. Response times may vary depending on the nature of the complaint but the DPO will endeavor to provide a response as promptly as possible and will update the complainant in the event of unexpected delays.

The DPO will liaise with any relevant teams or departments within the Firm and, where applicable, with any relevant third party service providers to investigate the matter. Where the complaint concerns a potential data security incident such as suspected loss or compromise of personal data, the Firm's security incident management procedures will also be initiated.

In every instance, the Firm will seek to ensure that the complainant is satisfied that the complaint is being dealt with promptly and seriously; receives a prompt response; receives an assurance that the issue is being reviewed; and is notified as soon as possible of the outcome.

The outcome of the investigation will be confirmed to the complainant in writing. In confirming the outcome, the DPO will set out the actions the firm proposes to take where a complaint is upheld or otherwise remind the complainant of the right to appeal if the complaint is rejected. If the individual feels that their complaint has not been satisfactorily resolved, they may appeal to the General Counsel for Norton Rose Fulbright US LLP who will review the outcome reached by the DPO and provide a decision based on their findings within 3 calendar months of receipt of the appeal.

The Firm's approach whenever data protection concerns are raised is to engage positively to try to resolve a complaint satisfactorily and to reach an understanding with the complainant without the individual needing to escalate matters or having to refer their complaint to an external data protection regulator or court.

Managing Data Subject Access Requests

Norton Rose Fulbright US LLP, (**the Firm**), recognizes that it may from time to time receive requests from individuals seeking to exercise their right of access and/or the other data subject rights provided by applicable data privacy laws such as the California Consumer Privacy Act (**CCPA**).

Norton Rose Fulbright US LLP will, as indicated in its Data Protection Policy, respect the legal rights individuals have, whose personal data is held by the firm, in relation to the processing of that personal data.

The firm will generally respond to a Data Subject Access Request (**DSAR**) promptly and in any event within 45 days of receiving the request (or, where applicable, upon receiving the requisite additional information/formalities as described below) unless local law stipulates otherwise or an extension of up to an additional 45 days is required (and permitted by the CCPA) due to the complexity of the request. We will acknowledge receipt of your request within 10 days.

The firm's Data Protection Officer for United States (**DPO**) in conjunction with its General Counsel are responsible for responding to a DSAR. A high-level overview of how the firm manages a DSAR is set out below.

Initial receipt and acknowledgment of request

The firm recognizes that a valid DSAR does not need to explicitly refer to the CCPA or include the words "data subject access request". It is sufficient that the request is in writing and makes clear that the individual wishes to know whether the firm holds personal data about them (for example a personnel file) and requests access to or a copy of that data. As such, the firm appreciates that such requests may come from past, current or potential NRF personnel, or from clients, suppliers, or anyone else whose personal data is stored by the firm.

DSARs will typically be sent by an applicant to a member of the firm's HR team or the relevant Partner/Department Head and are then promptly (and in any event within 24 hours of receipt) forwarded to the DPO, and General Counsel. The DPO will initially respond within 10 days to the applicant in writing acknowledging receipt of the DSAR, indicating that they will manage the firm's response and reassuring the applicant that the firm is happy to make available the information held about them in accordance with their rights.

As part of this initial response, if the applicant is not a current employee or firm personnel, the DPO will request proof of identity (such as a copy of a passport or driving license if this has not been provided with the request or as part of the engagement letter process). Additionally, where the scope of information requested in a DSAR is vague or unclear, the DPO may either seek clarification to assist with locating the information (for example, querying whether the applicant is looking for a document or category of documents only or asking if there are particular individuals whose firm mailboxes may include relevant personal data) or set out the parameters and scope the firm will apply in searching for and retrieving the applicant's personal data.

Identifying and retrieving relevant information

Once the scope of a DSAR has been agreed, the DPO will work with the firm's IT security team and relevant other IT service teams to identify potentially relevant data stored in the firm's email and other IT systems/repositories. The DPO will also establish whether any relevant manual files/hard copy filing systems exist.

From an email perspective, key words searches using, for example, variations of the applicant's name, username, initials, date range and any other search terms specified in the request are run against the firm's email system. In line with good practice, the DPO will inform individuals whose mailboxes are identified as potentially holding relevant information that searches need to be run on their IT accounts because a DSAR has been received. The DPO will also confirm with these individuals whether potentially relevant material may be held in the local home area of their IT accounts and, if necessary, run checks for relevant documentation in this area.

Depending on the scope of the request, searches will also be run across the firm's other databases and information repositories such as its HR, payroll, learning and performance management, and document management systems and its rewards and benefits portal. Hard copy personnel files will also be retrieved and checks carried out to establish whether there are any hard copy notebooks or similar other items that may be regarded as relevant filing systems.

Review of information

Once the results from the various searches are available, these will be reviewed by the DPO. As an initial step, duplicates and "false positives" (i.e. instances of personal data of other individuals with the same first name or surname as the applicant) will be removed from the search results.

The remaining material will then be reviewed again to determine the information to which the applicant is entitled under the CCPA or equivalent local laws and whether any redactions need to be made. As part of this assessment, the DPO and General Counsel will consider whether any exemptions need to be applied (such as legal advice/litigation privilege, management forecasting, negotiations with the applicant, or third party data). In relation to examples involving third party data, where such data is intermingled with the applicant's personal data, the firm will typically contact the other individual to confirm whether they consent to the disclosure of their information to the applicant without redactions. Instances where sections of the material contain third party data only will usually be withheld unless the firm is satisfied that the third party data is of a sufficiently non-sensitive/anodyne nature.

Response to the applicant

It is the firm's policy to provide its DSAR response in an electronic format unless the applicant specifically requests a hard copy of the response (and to retain a further copy for its own records that is stored in accordance with its document retention practices). The firm will provide a covering letter alongside the bundle of documents comprising the DSAR response, which will re-iterate the facts of the request (e.g. date submitted, agreed scope) and set out the firm's approach in providing its response. If the response includes any redacted material, the letter will explain the exemptions applied when making these redactions.

The covering letter will also set out the other information to which an applicant is entitled under the CCPA or equivalent local laws This includes:

- a description of the personal data held (in instances where a copy of the original emails/documents containing the personal data has not been provided or where the full personal

data has not been extracted and provided separately when a copy of the entire/redacted original email/document has not been provided);

- the categories of personal data held and the purposes for which the firm processes the personal data;

- the source (where this is not already clear, for example in email correspondence) and the recipients of the personal data.

Managing follow-up queries

As indicated above, Norton Rose Fulbright US LLP recognizes the rights of individuals whose data is held by the firm. Accordingly the firm will always aim to respond to a DSAR in a suitably comprehensive manner that addresses the information requested by the applicant in full and meets its legal obligations. In the event that an applicant has any queries about the response, the firm's approach is to engage positively to resolve such questions without the need for an applicant to have to escalate the matter or refer their complaint to an external regulator or court/body.

California Privacy Notice - All California Personnel

Background/purpose

This notice explains how Norton Rose Fulbright US LLP ("NRFUS" or "we") will protect your personal information.

Policy

The personal information NRFUS collects. NRFUS may collect (in both paper or electronic format) and use personal information about you. Such personal information may include:

- Personal contact details
- Date of birth
- Employment history
- Identification number
- Government identification numbers such as social security number, driver's license number or other identification card number
- Salary and benefits information including marital and dependent status as needed to administer benefits
- Beneficiary and emergency contact information
- Expense information and travel information
- Job performance information
- Information held for health and safety purposes
- Other information about you that could be deemed sensitive personal information (e.g. race, ethnicity and health under certain data privacy laws)
- Information about your use of the firm's resources
- Administrative information such as your bank account number (e.g., for direct deposit)
- Education and training
- Employment records (including references, work history and proof of work eligibility)
- Travel reimbursement information
- Information relating to criminal convictions and offenses
- Information about your use of the firm's systems, networks and devices
- Video surveillance from CCTV systems.

Our purposes for using your personal information. NRFUS collects this information for business purposes related to your role and function in the firm and for human resources management, including:

- Recruitment
- Performance management
- Payroll and expense reimbursement
- Training
- Business continuity
- Administration of compensation and benefit programs
- Facilitating business transactions
- Complying with health and safety obligations
- Assessing qualifications for a particular job or task

- Data relating to leaves of absence, including sickness absence data, to comply with employment law
- Physical or mental health condition or disability status to ensure personnel safety in the workplace and provide appropriate workplace accommodations
- Race or ethnic origin for work permit purposes
- Protecting NRFUS, its personnel or the public against injury, theft, legal liability, fraud, abuse or other misconduct
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution
- Proper and appropriate use of firm resources including its IT and computer systems
- Gathering evidence in connection with disciplinary action or termination
- To comply with our legal obligations and in connection with legal claims
- We may be required under local labor and other laws (e.g., health and safety, anti-discrimination) to maintain records that can include sensitive personal information, such as government identifiers, information relating to health, maternity or parental leave, pension and retirement.

Updates or requests related to your personal information. If you want to review and correct your personal information, or if you have questions about it, please contact Human Resources (us.hr@nortonrosefulbright.com). You can review and correct part of your personal information yourself by logging in to Vista Self-Service. Please note, for various legal reasons, we may not be able to comply with your request (e.g., NRFUS may have a legal obligation to retain the data). NRFUS will not discriminate against you for exercising any of these rights.

Sharing your personal information. We share your personal information with member firms of the Norton Rose Fulbright verein as part of our regular reporting activities on firm performance, in the context of a business reorganization or group restructuring, for system maintenance support and hosting of data.

We may disclose your personal information to agents and contractors that provide services to us, including insurance and benefits companies, and consultants. We also may send your personal information to companies we have contracted with to operate various information systems or to process certain transactions (e.g., payroll services providers).

We will also take the necessary steps under applicable data protection laws to protect it.

We may share your personal information to regulatory authorities (including tax authorities), government agencies, parties (including the NRFUS' advisors) in legal proceedings involving NRFUS, and third parties with whom NRFUS may collaborate or engage in combinations.

We may also share your information:

- During emergency situations or where necessary to protect the safety of persons
- Where the personal information is publicly available
- If a combination occurs and the disclosure is necessary to complete the transaction.

We have disclosed your personal information for the business purposes described above during the preceding 12 months, but we do not sell your personal information. We do not sell personal information of minors under the age of 16.

Changes. We reserve the right to amend it from time to time and we encourage you to periodically review this Notice on Athena.

Complaints about our use of your personal information. If you have a concern or a question about how we have processed your personal information, you should first raise your concern or question with Human Resources (us.hr@nortonrosefulbright.com). In the event that Human Resources (us.hr@nortonrosefulbright.com) is unable to resolve the concern or question, you may call (713) 651-7777 or email privacypolicy@NortonRoseFulbright.com for assistance.